IPCT/GB 2003 / 0 0 4 3 7 7

10/531431

INVESTOR IN PEOPLE

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

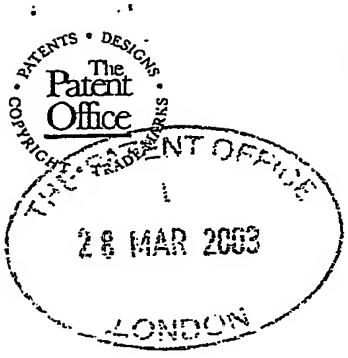
Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed J Evans.

Dated 26 November 2003

Patents Form 1/77

Patents Act 1977
(Rule 16)



[redacted]3 E796232-4 D02855
P01/7700 0.00-0307248.5

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference — 6/P40013GB

2. Patent application number *(The Patent Office will fill in this part)* — 0307248.5

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

VODAFONE GROUP PLC
VODAFONE HOUSE
THE CONNECTION
NEWBURY, BERKSHIRE
RG14 2FN

Patents ADP number *(if you know it)*

If the applicant is a corporate body, give the country/state of its incorporation — U.K.

8588251001

4. Title of the invention — FACILITATING AND AUTHENTICATING TRANSACTIONS

5. Name of your agent *(if you have one)*

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

MATHISEN, MACARA & CO.
THE COACH HOUSE
6-8 SWAKELEYS ROAD
ICKENHAM, UXBRIDGE
UB10 8BZ

Patents ADP number *(if you know it)* — 1073001 ✓

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*
U.K.	0224228.7	17 October 2002

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

YES

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	17
Claim(s)	10 DL
Abstract	1
Drawing(s)	4 4

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	
Request for preliminary examination and search *(Patents Form 9/77)*	1
Request for substantive examination *(Patents Form 10/77)*	
Any other documents *(please specify)*	Patents Form 1/77

11. I/We request the grant of a patent on the basis of this application.

Signature MATHISEN, MACARA & CO. Date 28th March 2003

12. Name and daytime telephone number of person to contact in the United Kingdom: MR M.C. FOSTER (01895 678331)

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

e) *Once you have filled in the form you must remember to sign and date it.*

f) *For details of the fee and ways to pay please contact the Patent Office.*

FACILITATING AND AUTHENTICATING TRANSACTIONS

The invention relates to the facilitation and authentication of transactions. In embodiments of the invention, to be described below in more detail by way of example only, transactions between data processing apparatus (such as a personal computer), or a user thereof, and a (possibly remote) third party are facilitated and authenticated, and such facilitation and authentication may also involve the facilitation and authentication of a payment to be made by or on behalf of the user to the third party.

According to the invention, there is provided a device for connection to a data processing apparatus, the device including means for operative coupling to authentication storage means storing predetermined information relating to the authentication of a transaction with the data processing apparatus, the device when operatively coupled to the data processing apparatus being responsive to an authentication process carried out via a communications link for authenticating the transaction, the authentication process involving the use of the predetermined information, and wherein the device controls access to the predetermined information.

According to the invention, there is also provided a method for authenticating a transaction with data processing apparatus in which the data processing apparatus has operatively associated with it a security device which in turn has operatively associated with it authentication storage means for storing predetermined authentication information,

and including the step of carrying out an authentication process via a communications link for authenticating the transaction, the authentication process involving the use of the predetermined authentication information obtained from the authentication storage means via the security device which controls access to the predetermined authentication information.

According to the invention, there is further provided a device for controlling access to authentication data stored on a authentication storage means, the device including means for coupling the device to a data processing apparatus to allow the authentication data to be used to authenticate a transaction performed by the data processing apparatus, wherein security means is provided for controlling access to the authentication data via the data processing apparatus.

A method according to the invention of facilitating and authenticating transactions involving data processing apparatus such as a personal computer, and devices for connection to data processing apparatus (such as a personal computer) embodying the invention, will now be described, by way of example only, with reference to the accompanying diagrammatic drawings in which:

Figure 1 is a block diagram for explaining the operation of the method in relation to the data processing apparatus;

Figure 2 is a flow chart for use in the understanding of the block diagram of Figure 1;

Figure 3 is a block diagram corresponding to Figure 1 in which a "dongle" in accordance with the invention is used; and

Figure 4 is a perspective view of one configuration of a dongle.

There exist many instances when a transaction involving the use of data processing apparatus requires authentication. For example, the data processing apparatus may be required to carry out a transaction, such as the exchange of information, with a third party, such as a remote third party with which the communication must be made over a telecommunications link (including via the Internet). The third party may require that the data processing apparatus, or the user thereof for the time being, is authenticated to the satisfaction of the third party before the transaction takes place.

As stated, the transaction may merely involve the exchange of information. For example, the user of the data processing apparatus may simply need to be authenticated in order to download information from the third party. Such information may be information kept by the third party on behalf of the user of the data processing apparatus (for example, information relating to the user's bank account). Instead, the information might be information held on other data processing apparatus, such as a data network belonging to an organisation or commercial entity with which the user is connected or by whom the

user is employed, thus facilitating access to that network by the user when the user is travelling. Another possible transaction may involve the downloading by the data processing apparatus of software from the remote location.

In addition, the transaction may require a payment to be made by the user in order to enable the transaction to take place, such as a payment to the third party in return for the information provided. Clearly, when such a payment is involved, it is important that the user is authenticated to the satisfaction of the third party and that the payment is made in a safe, simple and secure manner.

Although the foregoing discussion has referred to a "user" of the data processing apparatus, some at least of the transactions described above may not in fact involve any human user: the data processing apparatus may be required to operate automatically (for example, intermittently operating in an information-gathering or monitoring role, and reporting the results to a third party). In such cases, it may also be necessary for the data processing apparatus to authenticate itself to the satisfaction of the third party.

As described in our co-pending patent application No. GB 0224228.7, the data processing apparatus is provided with, or associated with, means (authentication storage means) for storing predetermined authentication information for authenticating that apparatus or a particular user thereof. In one embodiment, the means for storing the predetermined information is removable and can thus be taken by the user and inserted into any data

processing apparatus (or computer) which is adapted to receive it, so as to enable that user to be authenticated in respect to a transaction to be carried out by that user with that computer. Advantageously, in such a case the means for storing the predetermined information is in the form of a smart card.

In a more specific example, the smart card is a Subscriber Identity Module or SIM of the type used in and for authenticating the use of handsets in a cellular telecommunications network. Such a network will store details of its users' (subscribers') SIMs. In operation of the network, a user's handset is authenticated (for example, when the user activates the handset on the network with a view to making or receiving calls) by sending a challenge to the handset incorporating that SIM, in response to which the SIM calculates a reply (dependent on the predetermined information held on the SIM) and transmits it back to the network which checks it against its own information for that user or subscriber in order to complete the authentication process. In the same way, therefore, the SIM can be used in or in association with the data processing apparatus or computer so that the same form of authentication process can be carried out. In a case where the SIM is the SIM of a subscriber to a particular cellular telecommunications network, the authentication process can be carried out by that network.

It should be noted that the authentication process being described does not necessarily authenticate the human identity of the user. For example, cellular telecommunication networks have pre-pay subscribers who are issued with SIMs in return for pre-payment

enabling them to make calls on the network. However, the identity of such pre-pay subscribers is not known (or not necessarily known) by the networks. Nevertheless, such a user cannot make use of the network until the network has authenticated that user's SIM – that is, has confirmed that that user is a particular user who has a particular pre-paid account with the network. The SIMs of such pre-paid users or subscribers could equally well be used (in the manner described) in or in association with data processing apparatus or computers, for the purposes of authenticating that user.

The SIM need not take the form of a physical (and removable) smart card but instead can be simulated by being embedded in the data processing apparatus or computer in the form of software or represented as a chip for example.

It may be desirable to be able to change the authentication information on the SIM (or simulated SIM) to take account of changed circumstances. For example, the SIM may be a SIM registered with a particular cellular telecommunications network – a network applicable to the country or region where the data processing apparatus or computer is to be used. However, circumstances may arise (for example, the apparatus or the computer is physically moved to a different country or region) in which it is desirable or necessary to re-register the SIM with a different cellular telecommunications network. Ways in which this can be done are disclosed in our co-pending United Kingdom patent applications Nos. 0118406.8, 0122712.3 and 0130790.9 and in our corresponding PCT applications Nos. GB02/003265 and GB02/003260. As described therein in more detail,

a SIM (and thus also a simulated SIM) may be initially provided with authentication (and other) information relating to each of a plurality of networks, the information respective to the different networks being selectively activatable.

It is not necessary, however, for the users to be subscribers to a telecommunications network. Instead, they could be subscribers registered with some other centralised system which could then carry out the authentication process in the same way as in a telecommunications network. In such a case, the registration of a SIM (or simulated SIM) could be transferred from one such centralised system to another in the same manner as described above.

As described above, an aim of the authentication process is to facilitate a transaction between the data processing apparatus or computer and a third party. Where the authentication process is carried out by a telecommunications network, or by some other system, to which the user of the SIM is a subscriber, the satisfactory completion of the authentication process would then be communicated by that network or system to the third party – to enable the transaction to proceed.

For many transactions of the type described, a payment by the user to the third party may be involved. An arrangement as described above, in which the authentication process is carried out by a telecommunications network or other centralised system to which the user is a subscriber advantageously facilitates the making of such payments and is

particularly advantageous where (as may often be the case) the payment is for a small amount (for example, payment in return for receipt of information – e.g. weather or traffic information, or for temporary use of specific software); in such a case, the payment can be debited to the account of the subscriber held by the telecommunications network or other centralised system – and then, of course, passed on to the third party, perhaps after deduction of a handling charge.

The block diagram of Figure 1 explains one way of operating the method described above.

A Windows-based personal computer or PC 10 is shown ('Windows' is a trade mark). The PC10 is adapted to receive a SIM shown diagrammatically at 12. The SIM may be removably fitted to the PC, for use in identifying a user (that is, the holder of the SIM) or may be fixed within the PC (for identifying the PC itself). The PC 10 incorporates transaction management software 14 which interacts with and controls some of the functions of the SIM.

Also shown in Figure 1 is a cellular telephone network 16, such as the Vodafone (trade mark) network, and it is assumed that the SIM 12 is registered with the network 16.

The operation of the system shown in Figure 1 will be explained in relation to the flow chart of Figure 2.

At step A, the user of the PC 10 requests use of a particular application 17 on the PC. For example, the user might wish to view web pages containing specialised information which are encrypted and thus not generally available. In order to do this, the user requests a "session key" – that is, permission to carry out a transaction involving time-limited use of the particular application. The request for the session key is addressed to the transaction manager 14. The transaction manager 14 then, transmits identification information derived from the SIM 12 (an "I am here" message) to the security services part 18 of the network 16 (step B). In response to the "I am here" message, the network transmits a random challenge (step C) to the transaction manager 14, this challenge being based on information known to the network about the SIM 12.

At step D, the transaction manager 14 responds to the challenge by providing an answer derived from the challenge and the key held on the SIM. The reply is checked by the security services part 18 of the network 16. Assuming that the response is satisfactory, the security services part 18 authenticates the user and confirms this to the transaction manager 14 (step E). At the same time, the security services part 18 in the network transmits the session key (step F) to the application services part 22 of the network 16.

The transaction manager 14 also transmits the session key to the application 17 (step G).

The user can now make the request for the particular application (step H), accompanying

this application request with the session key received at step G. The application request of step H is transmitted to an application services part 22 which may be part of the network 16 (as shown) or may be separate and controlled by a third party. At step I the application services part compares the session key received with the application request (step H) with the session key received at step F. Assuming that the result of this check is satisfactory, the application services part 22 now transmits acceptance of the application request (step J) to the PC 10, and the application now proceeds (time limited). The network can now debit the user's account with a charge for the session.

The foregoing is of course merely one example of an implementation of what has been described.

In an alternative arrangement, a data carrier may be provided with means for storing predetermined information such as in one of the forms described above – that is, a SIM or (more probably) software simulating a SIM. The simulated SIM is associated with data stored on the data carrier. The data carrier may, for example, be a DVD or CD ROM or some other similar data carrier, and the data thereon may be software or a suite of software.

The simulated SIM may be used to identify and authenticate the data (such as the software) on the data carrier. The simulated SIM will be registered with a telecommunications network or some other centralised system, in the same manner as

described above. When the data carrier is placed in data processing apparatus such as a computer, for use therein, the SIM would be used to identify and authenticate the data carrier and the data stored thereon and (for example) could then permit the software to be downloaded for use in the computer. In this way, the SIM could be used subsequently to block further use of the software (for example, in another computer), or to allow the data to be used for only a predetermined number of times (whether in the same or in a different computer). If, for example, the data carrier (with its SIM) is placed in a computer which has also received a particular user's SIM then (a) the SIM on the data carrier can be used to identify and authenticate the software and (b) the SIM in or associated with the computer can be used to authenticate the user and could subsequently be used to enable a charge to be debited to that user as payment for use of the software.

According to the present invention, rather than the PC10 being adapted to receive a SIM 12, or a data carrier being modified to incorporate a SIM or software simulating a SIM, a separate device or "dongle" 30 is provided for receiving the SIM 12, or for incorporating software simulating the SIM 12.

The dongle 30 allows data for authenticating a transaction (or for any other appropriate purpose) to be passed between the dongle 30 and the PC 10 and onwardly to/from the network 16.

The dongle 30 comprises a plastics housing 32 having a slot for receiving a SIM 12.

Appropriate connectors (not shown) are provided within the housing 32 for allowing electronic exchange of data between the SIM 12 and the dongle 30. The dongle 30 further comprises a suitable connector 34 for allowing connection for data communication purposes to the PC 10. For example, the connector could be a USB connector, a Firewire 1394 connector or any other suitable connector. Of course, different configurations of the dongle may be provided. For example, the SIM 12 may be accommodated completely within the dongle 30, and may be removable from the dongle 30 by opening the housing 32, or the SIM 12 may be permanently sealed within the dongle casing 32. If the latter arrangement is provided, a user of the telecommunication system may be provided with a first SIM for use, for example, in their mobile telephone handset and may be provided with a dongle 30 which houses a separate SIM which is used for performing transactions via a PC 10. If desired, the telecommunications network will include a record indicating that the SIM within the user's mobile handset and the SIM within the user's dongle are commonly owned, and this information may be used to conveniently provide the user with a single account of charges incurred in respect of use of both the SIMs.

The dongle 30 is provided with a dongle interface driver 36 which controls communication with the PC 10. All communications from the PC10 are routed via the dongle interface driver 36 and data stored on the SIM 12 cannot be accessed other than by using the dongle interface driver 36. A corresponding PC interface driver 38 is provided for the PC 10. The PC interface driver 38 may, for example, comprise a series of commands in the form of a computer programme which is loaded onto and run by the PC

10. The PC interface driver 38 may, for example, be provided by or under the control of the network 16. The PC interface driver 38 will therefore be "trusted" by the network 16 and will be configured to only allow access to the dongle 30 and consequently the SIM 12 in an approved manner which will not allow the security information present on the SIM 12 to be compromised.

To prevent, or to reduce, the likelihood of the PC interface driver 38 being replaced or bypassed by an alternative driver, which could compromise the security of the data on the SIM 12, the PC interface driver 38 and the dongle interface driver 36 are provided with respective shared secret keys 40, 42. Each communication from the PC interface driver 38 to the dongle 30 is encrypted using the shared secret key 40. All communications from the PC 10 to the dongle 30 are received by the dongle interface driver 36. The dongle interface driver 36 comprises processing means for decrypting received communications using its secret key 42. To enhance security, the dongle interface driver 36 will prevent all communications other than those encrypted using the shared secret key 40 from sending data to or receiving data from the SIM 12.

Therefore, the PC interface driver 38 controls and supervises access to the dongle 30 and the SIM 12 to reduce the likelihood of the data stored on the SIM 12 being compromised by unauthorised attempts to access the SIM 12.

Provided that a request for access to data on the SIM 12 is approved by the PC interface

driver (according, for example, to criteria set by the network 16), and is therefore communicated to the dongle interface driver 36 with the appropriate key 40, a transaction can be authorised using the SIM 12 in the manner described in relation to Figures 1 and 2.

A further embodiment to the present invention will be described in relation to Figure 4. According to Figure 4, the dongle 30 has the SIM 12 accommodated completely within its housing 32, and the SIM cannot therefore be seen in the Figure. The dongle 30 has a connector 34 for connection to a PC 10 in a similar manner to the Figure 3 embodiment. At the opposite end of the casing 32 an optional loop connector 44 may be provided to provide a convenient means for carrying the dongle 30 by attaching it to a user's keyring.

One face of the housing 32 has a variety of push buttons 46 mounted thereon, ten of which have respective numerals from 0 to 9 displayed thereon. In this embodiment, the dongle 30 includes means (such as software) for receiving the entry of a PIN number from a user by operating the appropriately designated push buttons 46 which is compared to the PIN number provided for and stored on the SIM 12. The SIMs used in the GSM telecommunications network are conventionally provided with such a PIN.

The housing 32 may further optionally provide a display 48 for prompting the user to enter their PIN number and/or for displaying the PIN number as it is entered, if desired. On entry of the PIN number using the push buttons 46, the entered PIN number is compared to the PIN number stored on the SIM. If the PINs are found to match,

communication between the SIM and the PC10 is permitted to authorise one or more transactions. The comparison between the entered PIN number and the PIN number stored on the SIM 12 is performed within the dongle 30, and neither the entered PIN number nor the PIN number stored on the SIM is communicated to the PC10. This prevents or reduces the likelihood that the PINs will become compromised by disclosure to an authorised party.

The PIN entry comparison arrangement of Figure 4 may be provided in addition to or as an alternative to the interface drivers 36,38 and shared secret keys 40,42 of the arrangement shown in Figure 3.

It should be appreciated that as an alternative to push buttons 46, other means could be provided for allowing PIN entry. Alternatively, the user could be authorised to use the SIM by obtaining some other security information from the user and comparing this with data stored on the SIM 12. For example, the data obtained could be the user's fingerprint or some other characteristic which is unlikely to re-occur on another person. The details of the fingerprint (or other information) are stored on the SIM for comparison with the input data representing the characteristics.

As an additional security feature in the Figure 3 embodiment, a display may be provided which displays the name of the application or organisation which requests information from the SIM 12. This would allow the user to monitor requests being made to his SIM

12.

If the respective interface drivers 36,38 and shared secret keys 40,42 described in relation to Figure 3 are used in a system which also includes the PIN entry and comparison arrangement described in relation to Figure 4, to provide an added level of security, the dongle 30 can be programmed to display the name of the application or organisation requesting data from the SIM 12 and may then prompt the user to approve the supply of data for each or selected applications/organisations by entering the user's PIN using keypad 46.

The dongle 30 may be used to facilitate transactions with data processing apparatus other than PCs. For example, a user having an account with network 16 and being provided with a dongle 30 can insert the connector 34 into an appropriately configured slot in a parking meter which is connectable to the network 16. The SIM 12 contained within the dongle 30 is authenticated in the manner described above using a transaction manager provided within the parking meter. By this means, payment for parking can be made by deducting an appropriate amount from the user's account with the network 16. Advantageously, the dongle 30 will be provided with push buttons 46 and the dongle will prompt the user to enter a PIN which is compared to the PIN stored on the SIM so that the dongle 30 cannot be used by an unauthorised party. The dongle could be programmed to allow the push buttons 46, under control of the parking meter, to allow entry of data relevant to the transaction – for example, the length of time for which the parking space is

required.

The dongle 30 could, for example, also be used in a similar way with an appropriately configured DVD player to allow a film to be viewed on payment of a fee deducted from the user's account with the network 16.

CLAIMS

1. A device for connection to a data processing apparatus, the device including means for operative coupling to authentication storage means storing predetermined information relating to the authentication of a transaction with the data processing apparatus, the device when operatively coupled to the data processing apparatus being responsive to an authentication process carried out via a communications link for authenticating the transaction, the authentication process involving the use of the predetermined information, and wherein the device controls access to the predetermined information.

2. The device of claim 1, comprising security data entry means for obtaining security data independently of the data processing apparatus, and means for analysing the entered security data for determining whether to allow access to the predetermined information.

3. The device of claim 2, wherein the security data entry means comprises alphanumeric data entry means.

4. The device of claim 2 or 3, wherein the security data entry means comprises a keypad.

5. The device of claim 2,3 or 4, wherein the security data comprises a Personal

Identification Number (PIN) and the analysing means compares the PIN obtained by the security data entry means with a PIN stored on the authentication storage means and only allows access to the predetermined information when the respective PINs match.

6. The device of any one of the preceding claims, comprising a display for displaying security information.

7. The device of any one of the preceding claims, comprising a data processing module for controlling the communication with the data processing apparatus.

8. The device of claim 7, wherein the data processing module of the device is configured for communicating with a corresponding data processing module of the data processing apparatus.

9. The device of claim 8, wherein communication between the authentication storage means and the data processing apparatus is performed via the respective data processing modules.

10. The device of claim 7,8 or 9, wherein the data processing module of the device includes means for decrypting encrypted data received from the data processing module of the data processing apparatus.

11. The device of claim 7,8,9 or 10, wherein the data processing module of the device includes means for encrypting data transmitted to the data processing module of the data processing apparatus.

12. The device of claims 10 or 11, wherein the respective data processing modules comprise a key for allowing encryption and/or decryption of data.

13. The device of claim 12, wherein the key comprises a shared secret key for each of the respective data processing modules.

14. The device of any one of the preceding claims, wherein the device is operatively coupleable to one of more of a plurality of said authentication storage means, each of which is registerable with a common telecommunication system, and wherein the authentication process is performed by a communications link with the telecommunications system.

15. The device of claim 14, in which the predetermined authentication information stored by each authentication storage means corresponds to information which is used to authenticate a user of that authentication storage means in relation to the telecommunications system.

16. The device of claim 15, in which each user is authenticated in the

telecommunications system by means of the use of a smart card or subscriber identity module (e.g. SIM), and in which the authentication storage means respective to that user corresponds to or simulates the smart card for that user.

17. The device of any one of claims 1 to 16, in which the transaction is a transaction involving use of the data processing functions of the data processing apparatus.

18. The device of any one of claims 1 to 17, in which the authentication storage means is specific to that device.

19. The device of any one of claims 1 to 18, in which the authentication process involves the sending of a message and the generation of a response dependent on the message and the predetermined information.

20. The device of any one of claims 14 to 19, wherein the telecommunications system includes means for levying a charge for the transaction when authorised.

21. The device of any one of the preceding claims in combination with the data processing apparatus.

22. The device of any one of the preceding claims in combination with the telecommunications system.

23. A method for authenticating a transaction with data processing apparatus in which the data processing apparatus has operatively associated with it a security device which in turn has operatively associated with it authentication storage means for storing predetermined authentication information, and including the step of carrying out an authentication process via a communications link for authenticating the transaction, the authentication process involving the use of the predetermined authentication information obtained from the authentication storage means via the security device which controls access to the predetermined authentication information.

24. The method of claim 23, comprising obtaining security data independently of the data processing apparatus, and analysing the security data for determining whether to allow access to the predetermined information.

25. The method of claim 24, wherein the security data is obtained by alphanumeric data entry means.

26. The method of claim 23 or 24, wherein the alphanumeric data entry means comprises a keypad.

27. The method of claim 24,25 or 26, wherein the security data comprises a Personal Identification Number (PIN) and the analysing step compares the PIN obtained by the

security data entry means with a PIN stored on the authentication storage means and only allows access to the predetermined information when the respective PINs match.

28. The method of any one of claims 23 to 27, comprising displaying security information.

29. The method of any one of claims 23 to 28, wherein communication with the data processing apparatus is controlled by a data processing module.

30. The method of claim 29, wherein the data processing module of the device is configured for communicating with a corresponding data processing module of the data processing apparatus.

31. The method of claim 30, wherein communication between the authentication storage means and the data processing apparatus is performed via the respective data processing modules.

32. The method of claim 29,30 or 31, wherein the data processing module of the device decrypts encrypted data received from the data processing module of the data processing apparatus.

33. The method of claim 29,30, 31 or 32, wherein the data processing module of the

device encrypts data transmitted to the data processing module of the data processing apparatus.

34. The method of claims 32 and 33, wherein the respective data processing modules comprise a key for allowing encryption and/or decryption of data.

35. The method of claim 34, wherein the key comprises a shared secret key for each of the respective data processing modules.

36. A method according to any one of claims 23 to 35, wherein the security means is operatively associated with one or more authentication storage means of a plurality of authentication storage means each for storing predetermined authentication information, the authentication storage means being registerable with a common telecommunications system, and wherein the step of carrying out the authentication process is performed via a communications link with the telecommunications system.

37. A method according to claim 36, in which the predetermined authentication information stored by each authentication storage means corresponds to information which is used to authenticate a user of that authentication storage means in relation to the telecommunications system.

38. A method according to claim 37, in which each user is authenticated in the

telecommunications system by means of the use of a smart card or subscriber identity module (e.g. SIM), and in which the authentication storage means respective to that user corresponds to or simulates the smart card for that user.

39. A method according to any one of claims 37 to 38, in which the transaction is a transaction involving use of the data processing functions of the data processing apparatus.

40. A method according to any one of claims 23 to 39, in which each authentication storage is associated with a specific security device.

41. A method according to any one of claims 23 to 40, in which the authentication storage means is associated with the data processing apparatus by being associated with data or software for use by that data processing apparatus.

42. A method according to any one of claims 23 to 41, in which the authentication process involves the sending of a message and the generation of a response dependent on the message and the predetermined information.

43. A method according to any one of claims 23 to 42, including the step of levying a charge for the transaction when authenticated.

44. A method according to claim 43, in which the step of levying the charge is carried out by the said telecommunication system.

45. A method according to any one of claims 23 to 44, in which the data processing apparatus is a personal computer.

46. A device for controlling access to authentication data stored on a authentication storage means, the device including means for coupling the device to a data processing apparatus to allow the authentication data to be used to authenticate a transaction performed by the data processing apparatus, wherein security means is provided for controlling access to the authentication data via the data processing apparatus.

47. The device of claim 46, wherein the security means comprises means for obtaining security data from a user and means for checking the validity of the security data and only allowing access to the authentication data if the security data is valid.

48. The device of claim 46 or 47, wherein the security means comprises data processing means for receiving an encrypted authentication request, encrypted using a predetermined key, from the data processing apparatus and for decrypting the request.

49. The device of claim 48 in combination with the data processing means, wherein the data processing means comprises means for encrypting the authentication request

using said key.

50. A method for authenticating a transaction with data processing apparatus, substantially as described with reference to the accompanying drawings.

51. A device substantially as described with reference to the accompanying diagrammatic drawings.

ABSTRACT (Figure 3)

A device or "dongle" (30) is provided for controlling communications between a Subscriber Identity Module (or SIM) (12), such as of the type used in a GSM cellular telephone system, and a computer, such as a Windows-based PC (10). The SIM (12) can be authenticated by the telephone network, in the same way as for authenticating SIMs of telephone handset users in the network, and can in this way authenticate the user of the PC (10) or the PC (10) itself. Such authentication can, for example, permit use of the PC (10) for a time-limited session in relation to a particular application which is released to the PC (10) after the authentication is satisfactorily completed. The application may be released to the PC (10) by a third party after and in response to the satisfactory completion of the authentication process. A charge for the session can be debited to the user by the telecommunications network and then passed on to the third party. The dongle (30) provides additional security for the authentication data stored on the SIM by requiring a PIN to be entered and/or by only being responsive to requests received from the PC (10) which are encrypted using a key, which requests are generated by a special PC interface driver (38).

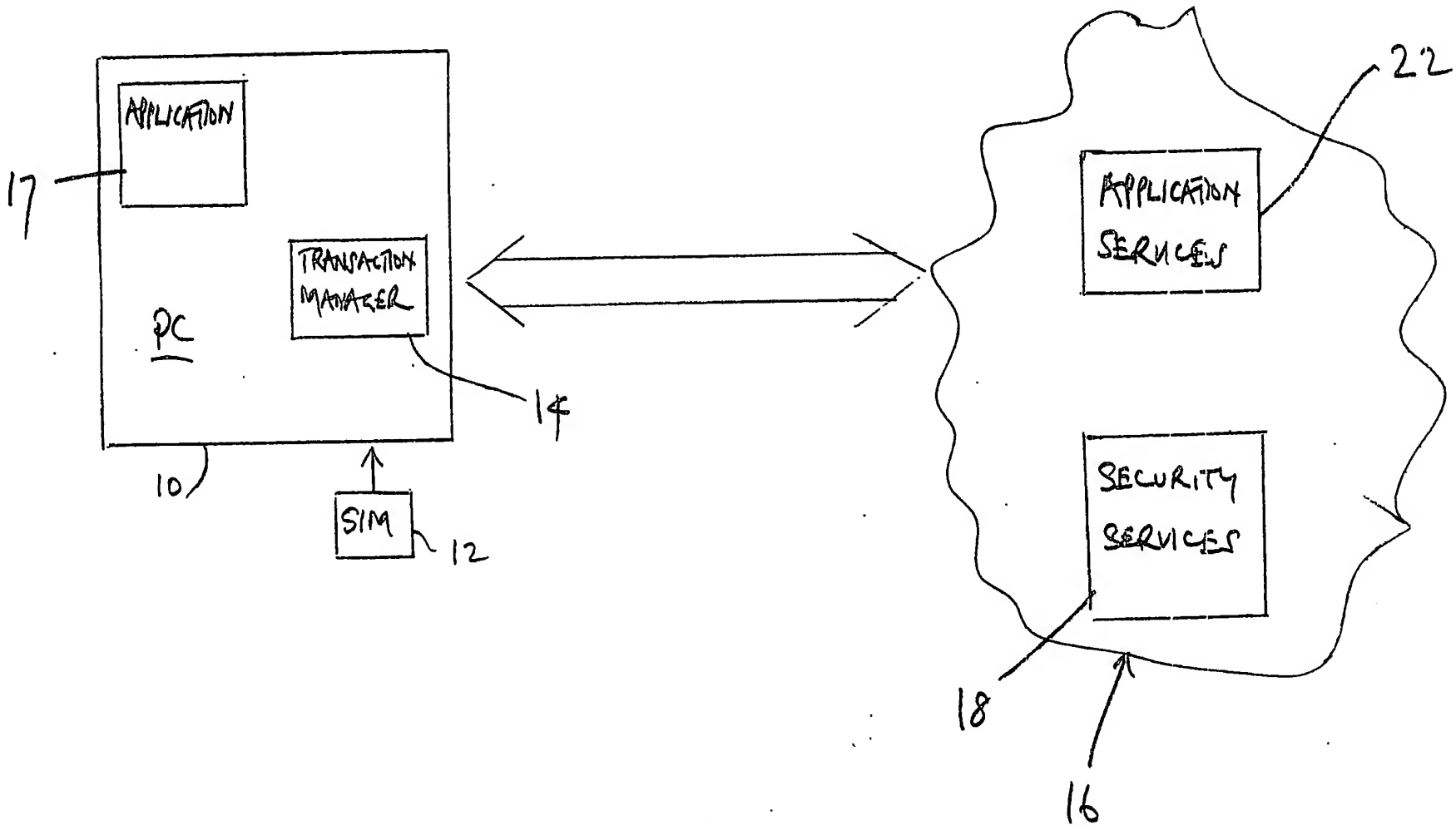

APPLICATION
17
TRANSACTION MANAGER
PC
14
10
SIM
12
22
APPLICATION SERVICES
SECURITY SERVICES
18
16

Fig. 1

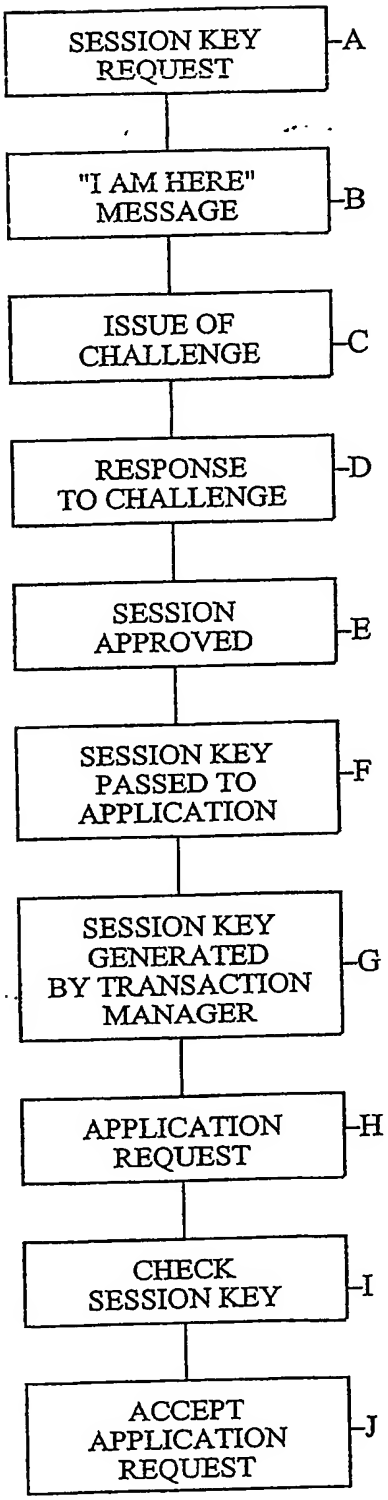

SESSION KEY REQUEST
A
"I AM HERE" MESSAGE
B
ISSUE OF CHALLENGE
C
RESPONSE TO CHALLENGE
D
SESSION APPROVED
E
SESSION KEY PASSED TO APPLICATION
F
SESSION KEY GENERATED BY TRANSACTION MANAGER
G
APPLICATION REQUEST
H
CHECK SESSION KEY
I
ACCEPT APPLICATION REQUEST
J

Fig. 2

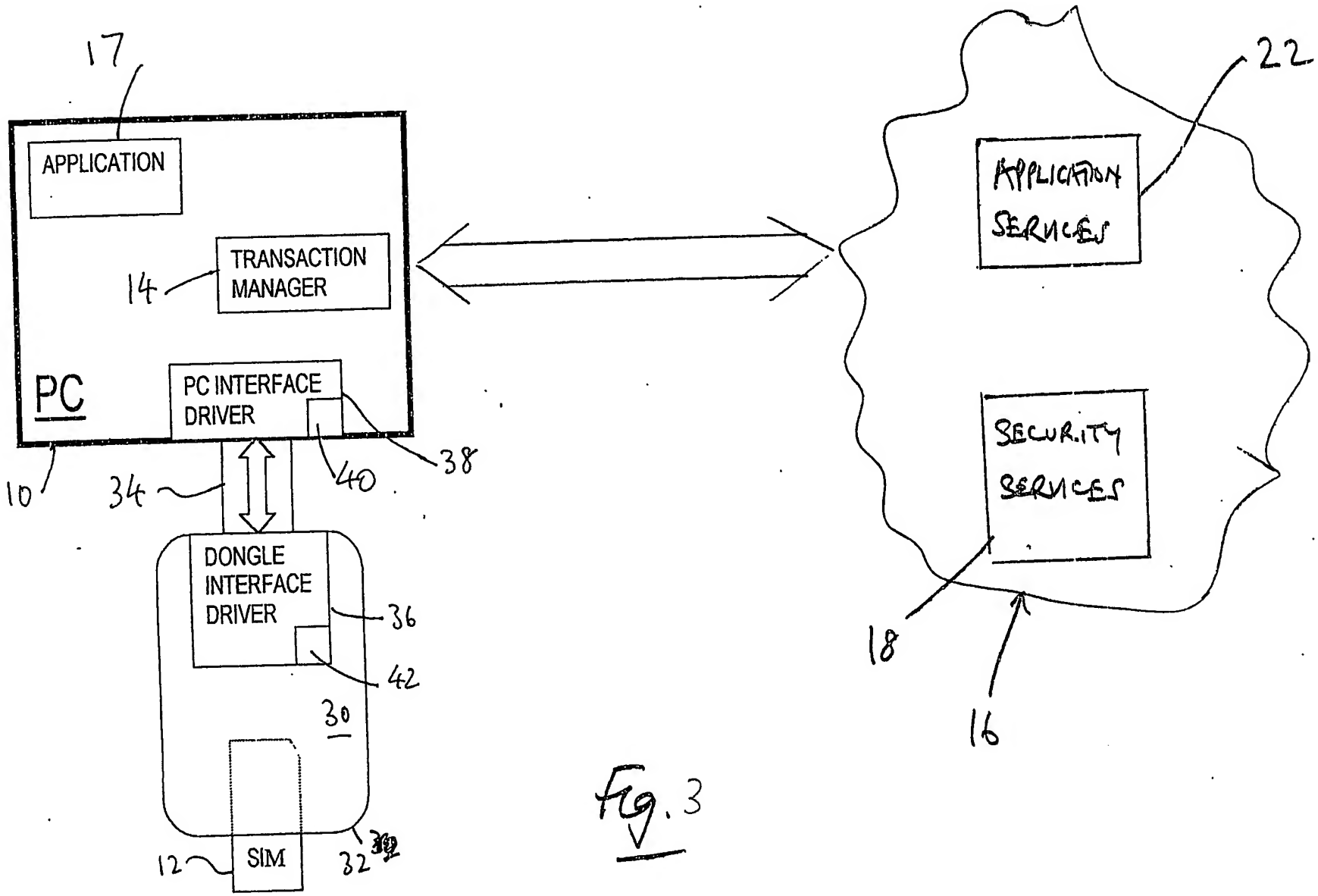

17
APPLICATION
TRANSACTION MANAGER
14
PC
PC INTERFACE DRIVER
10
34
40
38
DONGLE INTERFACE DRIVER
36
42
30
SIM
12
32
22
APPLICATION SERVICES
SECURITY SERVICES
18
16

Fig. 3

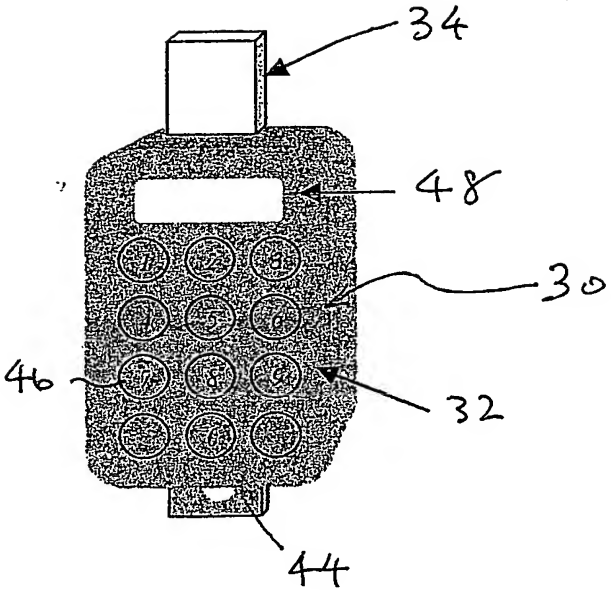


Fig. 4